PATENT APPLICATION
DOCKET NO. 100201141-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTOR(S): Gregory Eugene Perkins, et al.

SERIAL NO.: 10/085,927 **GROUP ART UNIT**: 2141

FILED: Feb. 27, 2002 **EXAMINER:** Bayard, Djenane M

SUBJECT: RESOURCE LOCATION AND ACCESS

APPELLANTS'/APPLICANTS' REPLY BRIEF ON APPEAL

The Appellants filed a first appeal brief on June 27, 2006. The Examiner responded reopening prosecution with a new ground for rejection. The Appellant filed a second opening brief addressing the new grounds on April 16, 2007. The Examiner again responded by reopening prosecution with a new ground for rejection. Again, the Appellant addressed the new grounds for rejection in a third brief filed February 25, 2008. The Examiner has responded to the third opening brief in an answer submitted April 16, 2008. The Following is a reply to the Examiner's Answer.

1. **Grounds For Rejection To Be Reviewed.**

A. Claims 9 and 13-15 stand rejected under 35 USC §101 as being directed to non-statutory subject matter.

B. Claims 1, 2, 5, 9-10, 13, 17-25 stand rejected under 35 USC §102 as being anticipated by USPN 6,490,624 issued to Sampson.

C. Claims 3 and 11stand rejected under 35 USC §103 as being unpatentable over Sampson in view of US Pub 2003/0074580 to Knouse.

D. Claims 4 and 12 stand rejected under 35 USC §103 as being unpatentable over Sampson in view of Knouse and in further view of USPN 2004/0015580 to Lu.

E. Claims 6 and 14 stand rejected under 35 USC §103 as being unpatentable over Knouse and in further view of Lu.

F. Claims 7 and 15 stand rejected under 35 USC §103 as being unpatentable over Sampson in further view of Lu.

2. **Argument.**

Grounds For Rejection A – Claims 9 and 13-15 stand rejected under 35 USC §101 as being directed to non-statutory subject matter.

It is initially noted that the grounds for rejecting Claims 9 and 13-15 as explained in the Examiner's answer at page 14 is new. For the first time in the Answer, the Examiner refers to the Specification to explain a new basis for the §101 rejection. In particular, the Examiner now explains that the Specification, paragraph [0033], defines

computer readable medium to include carrier waves in the form of infrared and/or electromagnetic media.

In the most recent office action mauled July 31, 2007, the Examiner at page 2 explained the rejection as follows:

> Claims 9, 12 - 5 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a computer-readable medium, in a computer, on an electromagnetic carrier signal does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8.

Until now the Examiner has made no reference to the Specification. Had the Examiner made this new rejection earlier, the Appellant would have gladly amended the Specification accordingly. Should the case be remanded to the Examiner, the Appellant would gladly make such an amendment.

Nonetheless, the Applicants arguments with respect to the basis for the rejection explained in the July 31 office action stand.

Grounds For Rejection B – Claims 1, 2, 5, 9-10, 13, 17-18, and 20-25 stand rejected under 35 USC §102 as being anticipated by USPN 6,490,624 issued to Sampson.

Claim 1 is directed to a method for locating a resource and expressly recites the provision of a user interface that has instructions to send association data. That association data is then used to identify an identity service that manages resource data. A resource is located using the resource data. In the third opening brief, the Appellant explained that Sampson failed to teach or suggest a method that includes (a) identifying an identity service using the association data, the identity service managing resource data or (b) locating the resource using the resource data.

With respect to the act of identifying an identity service using the association data, the Examiner responded at page 15 of the Answer stating:

> Sampson clearly teaches wherein the browser sends a cookie (association data) to a protected web server (identity service) which is a web server with resources (See col. 7, lines 64-66). It is well known to one with ordinary skill in the art, as stated by Sampson (See col. 7, lines 56-58) "cookies received from a web server in a specific domain are returned to web servers in that same domain during URL request". Therefore, it would have been obvious that the cookie of Sampson is used to identify the Protected Web server when the user selects a request since the cookie is returned to the web server and is required for access to resources protected by the system (See col. 7, lines 56-66).

Initially it is noted that the Examiner rejected Claim 1 under §102 as being anticipated by Sampson. The Examiner's response reproduced above is directed to a §103 obviousness rejection. Nonetheless, even if Sampson's cookie is used to identify a protected web server, the protected web server is NOT an identity service that manages resource data.

Paragraph [0022] of the Specification states that an identity service is "any combination of hardware and/or programming capable of providing information for locating and accessing resource service 14." The same paragraph explains that the "resource service 14 represents any combination of hardware and/or programming capable of providing a resource to a distributed application." Thus, the information for locating the resource service is the resource data recited by Claim 1. Paragraph [0031] states that resource data can includes the network address and a description of a given resource. The resource data "may **also** include any credentials such as a user name and password needed to access the resource." Paragraph [0031] (emphasis added). The term "also" indicates that in addition to including the network address of the resource, the resource data may include credentials. Such is consistent with the exemplary resource data described in paragraph [0026] where the resource data is shown as an URL that includes the network address of a resource as well as credentials for accessing the resource.

Sampson's cookie is not used to identify an identity service that manages resource data. Instead, Sampson explains:

> When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. The cookie is also used by the resource to return information that is customized based on the user's name and roles.

Sampson, col. 7, line 64 through col. 8, line 4. In other words, Sampson teaches that the cookie is used by a runtime module to verify that the user is authorized to access the resource and used by the resource to return information that is customized based on the user's name and roles. Sampson's protected web server is not an identity service that manages resource data.

With respect to the Appellant's explanation that Sampson fails to teach locating a resource using the resource data, the Examiner, at page 15 of the Answer states:

> Appellant's disclosure recites" Resource data may include the network address and a description of each resource. It may also include any credentials such as a user name and password needed to access the resource" (See pages 7 and 8, paragraph [0031]). Sampson teaches wherein the Runtime module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource (See col. 7, line 67 and col. 8, lines 1-2).

The Examiner is misconstruing Claim 1. Initially the Examiner is asserting that Sampson cookie is the association data used to identify the identity service that manages the association data. The Examiner now goes on to argue that the same cookie is also the resource data used to identify the resource. Tin other words, the Examiner is equating the cookie with the recited association data as well as the recited resource data. Plainly this is not the case. The Appellant questions why would Sampson's cookie be used to identify identity service that manages the cookie itself and then use the cookie to identify the resource?. Plainly the recited resource data is not the cookie that served as the association data.

Moreover, the recited resource data, according to paragraph [0031] of the Specification is "data used to locate and access a resource. Thus it serves two

purposes – locating and accessing. If the resource is not protected, the network address of the resource may be sufficient to locate and access the resource. If the resource is protected, the network address as well as credentials may be needed. In other words, the recited resource data will include some form of information such as a network address for locating the resource. In addition to that locating information, the resource data may ALSO include credentials needed to access the resource. The resource data always includes more than credentials – it includes information, such as a network address, for locating the resource.

The Examiner asserts that Sampson's cookie is used for authorization and is apparently implying that the cookie includes credentials. As explained , the inclusion of credentials alone is insufficient to equate Sampson's cookie with the recited resource data.

Consequently, Sampson fails to teach a method that includes (a) identifying an identity service using the association data, the identity service managing resource data, or (b) locating the resource using the resource data. For at least this reason, Claim 1 is patentable over Sampson. Claims 2-4 are also patentable over Sampson due at least in part to their dependence from Claim 1.

Claim 5 is directed to a method for locating a resource for a user and recites the following acts:

1. providing an interface having instructions to send association data to two or more association services;
2. identifying from the two or more association services, an association service with which the user has established a relationship;
3. identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and
4. locating the resource using the resource data.

As with Claim 1, Sampson fails to teach or suggest (a) using association data to identify an identity service that manages resource data or (b) locating a resource using that resource data. For at least the same reasons Claim 1 is patentable over Sampson, so is Claim 5.

Claim 5 also recites providing an interface having instructions to send association data to two or more association services. The Examiner asserts this is taught by Sampson col. 13, lines 1-10 and col. 14, lines 44-52. The Examiner equates the cookie with the recited association data. The cited passages mention nothing of sending different cookies to different two or more association services.

Moreover, Claim 5 recites "identifying from the two or more association services, an association service with which the user has established a relationship." The Examiner asserts this is taught by Sampson, Col. 13, lines 6-17. The passage relied upon by the Examiner is reproduced below:

> The Session Manager object takes the Session ID and performs checks on it. For example, as shown in block 532 , the Session Manager object checks to determine whether the Session ID is recognized or known, by searching a local hash table of the Session Manager object to find the Session ID. If the Session ID is not found in the local hash table, then an internal error is generated, and a login page is returned to Client 100 , as indicated by block 533 . Thereafter, to gain access to the Protected Server, the Client 100 must provide valid usemame and password information through the login page to the Access Server. This prevents malicious users or processes from entering the system using an invalid Session ID.

Sampson, col. 13, lines 6-17.

The cited passage mentions nothing of association services let alone identifying a particular association service a user has a relationship with from among two or more association services.

Claim 9 is directed to a computer readable medium having instructions for implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so are Claim 9 and Claims 10-12 which depend from Claim 9.

Claim 13 is directed to a computer readable medium having instructions for implementing the method of Claim 5. For at least the same reasons Claim 5 is patentable, so is Claim 13.

Claim 17 is direct to a system capable of implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 17 and Claim 18 which depends from Claim 17.

Claim 19 is directed to a document production system and recites the following elements:

1. an association module operable to query an association service, supplying a session identifier in order to identify an identity service managing resource data; and
2. a document production application operable to:
3. provide an interface having content for sending association data containing a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;
4. acquire resource data from an identity service identifier identified by a query from the association module;
5. locate and access a document management service using the resource data; and
6. provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and
7. produce a document according to selections made through the interface.

The Examiner asserts that the association module element of Claim 19 is taught by Sampson, col. 13, lines 1-17. The cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches an association module as that element is recited in Claim 19. More particularly Sampson fails to teach or suggest "an association module operable to query an association service, supplying a session identifier in order to identify an identity service managing resource data." For at least this reason, Claim 19 is patentable over Sampson.

Claim 20 is directed to a system for locating a resource and recites the following elements:

1. an identity service operable to manage resource data;
2. an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;
3. an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using a session identifier supplied with the query;
4. an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;
5. an application operable to:

6. provide an interface having instructions to send association data to an association server, the association data to contain a client identifier and a session identifier for the provided interface;
7. acquire resource data from the identity service identified by a query from the association module; and
8. locate the resource using the resource data.

The Examiner asserts that the association module element of Claim 20 is taught by Sampson, col. 13, lines 6-13 stating "the session manager object checks to determine whether the session Id is recognized or known."

As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches an association module as that element is recited in Claim 20. More particularly Sampson fails to teach or suggest an "association module operable to query, supplying a session identifier, the association service in order to identify the identity service." For at least this reason, Claim 20 is patentable over the cited references as is Claim 21 which depends from Claim 20.

Claim 22 is directed to a document production system and recites the following elements:

1. a document management service;
2. an identity service operable to manage resource data for locating and accessing the document management service;

3. an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;
4. an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using the session identifier supplied with the query;
5. an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;
6. a document production application operable to:
7. provide an interface having content for sending association data containing a client identifier and a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;
8. acquire resource data from an identity service using the session identifier for the identity service identified by a query from the association module;
9. locate and access the document management service using the resource data;
10. provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and
11. produce a document according to selections made through the interface.

The Examiner asserts that the association module element of Claim 20 is taught by Sampson, col. 13, lines 1-17. As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must

re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches an association module as that element is recited in Claim 20. More particularly Sampson fails to teach or suggest an "association module operable to query, supplying a session identifier, the association service in order to identify the identity service." For at least this reason, Claim 22 is patentable over Sampson as is Claim 23 which depends from Claim 22.

Claim 24 is directed to a system for implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 24.

Claim 25 is directed to a document production system that includes the following:

1. a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data;
2. a means for providing an interface having content for sending association data containing a session identifier for the provided interface to the association service as well as content for displaying controls for selecting production options;
3. a means for acquiring resource data from an identity service identifier identified by a query;
4. a means for locating and accessing a document management service using the resource data;
5. a means for providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and
6. a means for producing a document according to selections made through the interface.

The Examiner asserts that the means for querying is taught by Sampson, col. 13, lines 1-17. As discussed above with respect to Claim 5, the cited passage explains that Sampson's session manager takes the Session ID and performs a series of tasks that include ensuring that the Session ID is in a hash table. Sampson, col. 13, lines 6-18. Sampson's Session ID is not used to identify an identity service that manages resource data. It is not even used to identify the protected server to which a client is requesting access. It is simply used to determine whether or not a client must re-enter a user name and password to access the protected server. Sampson, col. 13, lines 6-18 and Fig. 5C.

Nothing in Sampson teaches a means for querying as that element is recited in Claim 20. More particularly Sampson fails to teach or suggest "a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data." For at least this reason, Claim 25 is patentable over Sampson.

Grounds For Rejection C – Claims 3 and 11 stand rejected under 35 USC §103 as being unpatentable over Sampson in view of US Pub 2003/0074580 to Knouse.

Claim 3 depends from Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 3.

Claim 11 depends from Claim 9. For at least the same reasons Claim 9 is patentable, so is Claim 11.

Grounds For Rejection D – Claims 4 and 12 stand rejected under 35 USC §103 as being unpatentable over Sampson in view of Knouse and in further view of USPN 2004/0015580 to Lu.

Claim 4 depends from Claim 1. For at least the same reasons Claim 1 is patentable, so is Claim 4.

Claim 12 depends from Claim 9. For at least the same reasons Claim 9 is patentable, so is Claim 12.

Grounds For Rejection E – Claims 6 and 14 stand rejected under 35 USC §103 as being unpatentable over Knouse and in further view of Lu.

Claim 6 is directed to a method, in a computer network, for locating a resource and recites the following acts:

1. providing a web page having instructions to request a web bug;
2. requesting the web bug sending a cookie and an URL for the web page;
3. saving the cookie and the URL for the web page as an entry in an association table;
4. querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL;
5. identifying other entries in the association table containing the cookie;
6. identifying from those entries an entry containing an URL for an identification service, the identification service managing resource data; and
7. locating the resource using the resource data.

In the third opening brief, the Appellant explained that Knouse and Lu fail to teach or suggest (a) saving the cookie and the URL for the web page as an entry in an association table and (b) querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL identifying an identity service using the association data. At page 20 of the Answer the Examiner responded citing Knouse paragraphs [0207] and [0209].

Paragraph [0207] indicates that a number of protected domains can reside on the same web server. When the user is authenticated to a preferred host domain residing on the server as indicated by a cookie, the user is authenticate to all the domains residing on the server. Paragraph [0209] indicates that when the user is properly

authenticated to the master domain, the user is provided with a cookie and redirected to the requested protected domain. The redirection URL also includes the cookie. Thus when redirected, the cookie is stripped from the URL and used to prove that the user is already authenticated.

The Appellant respectfully maintains that the cited paragraphs mention nothing of an association table let alone saving a cookie and an URL as an entry in an association table. According to paragraph [0027] of the specification, an association table is a logical memory area used to store association data. Paragraph [0029] explains that the association table includes entries each having a client identifier and a session identifier. The recited association data of Claim 6 is the client identifier and the recited URL for the web page associated with the web bug is the session identifier.

The passages from Knouse relied upon by the examiner mention nothing of such an association table let alone querying the association table providing the URL for the web page associated with the web bug.

For the reasons set forth in the third opening brief, the Appellant maintains that Knouse and Lu also fail to teach the remaining limitation of Claim 6

These paragraphs mention NOTHING of identifying from those entries an entry containing an URL for an identification service, the identification service managing resource data.

For at least these reasons, Claim 6 is patentable over Knouse and Lu.

Claim 14 is direct to is directed to a computer readable medium having instructions for implementing the method of Claim 6. For at least the same reasons Claim 6 is patentable, so is Claim 14.

Grounds For Rejection F – Claims 7 and 15 stand rejected under 35 USC §103 as being unpatentable over Sampson in further view of Lu.

Claim 7 is directed to a method for producing an electronic document and recites the following acts:

1. generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;
2. querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;
3. obtaining the user's resource data from the identified identity service;
4. locating and accessing a document management service using the resource data;
5. providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and
6. producing a document according to selections made through the web page.

The Examiner asserts that the act of querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page is taught by Sampson, col. 7, lines 16-20 and col. 7, line 64 through col. 8, line 5. Those passages is reproduced as follows:

> If the login attempt is successful, the system 2 presents the User with a Personalized Menu that assists the User in identifying and selecting a Resource. In one embodiment, a Personalized Menu is an HTML page containing a list of authorized Resources. The Personalized Menu displays only Resources to which the User has access. The User can then select and access a Resource.

Sampson, col. 7, lines 16-22.

> When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The

> Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. The cookie is also used by the resource to return information that is customized based on the user's name and roles.

Sampson, col. 7, line 64 through col. 8, line 5.

The first passage describes presenting a user with a personalized menu in the form of an HTML page that contains a list of authorized resources. According to the second passage, when the user selects a resource from that HTML page, a cookie is sent to a web server that is protected by a run time module. The run time module decrypts the cookie to ensure that the user is authorized to access the resource.

Nothing in this passages teaches, suggests or even hints at a method that includes querying an association service to identify an identity service with which the user is registered by providing an URL for a generated web page as recited by Claim 7. More particularly, the passage is completely unrelated to "querying the association service to identify an identity service or any other service for that matter.

Lu is silent on this point.

For at least these reasons, Claim 7 is patentable over Sampson and Lu as is Claim 8 which depends from Claim 7

Claim 15 is directed to a computer readable medium having instructions for implementing the method of Claim 7. For at least the same reasons Claim 7 is patentable, so are Claim 15 and Claim 16 which depends from Claim 15.

Conclusion: In view of the foregoing remarks, the Applicant respectfully submits that the pending claims are in condition for allowance. Consequently, early and favorable action allowing these claims and passing the application to issue is earnestly solicited.

Respectfully submitted,
Gregory Eugene Perkins, et al.

By __/Jack H. McKinney/_____
Jack H. McKinney
Reg. No. 45,685

June 16, 2008

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. (original) In a computer network, a method for locating a resource, comprising:

providing an interface having instructions to send association data;

identifying an identity service using the association data, the identity service managing resource data; and

locating the resource using the resource data.

2. (original) The method of Claim 1, further comprising performing a specified task utilizing the resource.

3. (original) The method of Claim 1, wherein the association data includes a client identifier and a session identifier associated with the interface, and wherein the act of identifying comprises:

providing the session identifier associated with the interface, identifying the client identifier included in the association data;

identifying other association data containing that client identifier; and

acquiring at least a portion of the session identifier included in the other association data.

4. (original) The method of Claim 1, wherein the act of providing comprises providing a web page having instructions to request a web bug sending association data containing a cookie and an URL for the web page; and

wherein the act of identifying comprises:

providing the URL to identify the association data containing the cookie;

identifying other association data containing the cookie; and

acquiring an URL for the identity service from the identified association data.

5. (original) In a computer network, a method for locating a resource for a user, comprising:

providing an interface having instructions to send association data to two or more association services;

identifying from the two or more association services, an association service with which the user has established a relationship;

identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and

locating the resource using the resource data.

6. (original) In a computer network, a method for locating a resource comprising:

providing a web page having instructions to request a web bug;

requesting the web bug sending a cookie and an URL for the web page;

saving the cookie and the URL for the web page as an entry in an association table;

querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL;

identifying other entries in the association table containing the cookie;

identifying from those entries an entry containing an URL for an identification service, the identification service managing resource data; and

locating the resource using the resource data.

7. (original) A method for producing an electronic document, comprising:

generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;

querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;

obtaining the user's resource data from the identified identity service;

locating and accessing a document management service using the resource data;

providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and

producing a document according to selections made through the web page.

8. (original) The method of Claim 7, wherein:

the act of generating comprises generating a web page having instructions to request a web bug sending, to the association service association, data containing a cookie and an URL for the web page;

the method further comprises saving the association data as an entry in an association table;

the act of querying further comprises identifying the cookie in the saved entry using the provided the URL, identifying other association data containing the identified cookie, and, from the other identified association data, acquiring an URL for the identity service; and

the act of obtaining the user's resource data comprises obtaining the user's resource data from the identified identity service using, at least in part, the acquired URL.

9. (original) A computer readable medium having instructions for:

providing an interface having instructions to send association data;

identifying an identity service using the association data, the identity service managing resource data; and

locating a resource using the resource data.

10. (original) The medium of Claim 9, having further instructions for performing a specified task utilizing the resource.

11. (original) The medium of Claim 9, wherein the association data includes a client identifier and a session identifier associated with the interface, and wherein the instructions for identifying comprise instructions for:

providing the session identifier associated with the interface, identifying the client identifier included in the association data;

identifying other association data containing that client identifier; and

acquiring the session identifier included in the other association data.

12. (original) The medium of Claim 9, wherein the instructions for providing comprise instructions for providing a web page having instructions to request a web bug sending association data containing a cookie and an URL for the web page; and

wherein the instructions for identifying comprise instructions for:

providing the URL to identify the association data containing the cookie;

identifying other association data containing the cookie; and

acquiring, from the identified association data, an URL for the identity service.

13. (original) A computer readable medium having instructions for:

providing an interface having instructions to send association data to two or more association services;

identifying from the two or more association services, an association service with which a user has established a relationship;

identifying an identity service using the association data sent to the identified association service, the identity service managing resource data; and

locating a resource for the user using the resource data.

14. (original) A computer readable medium having instructions for:

providing a web page having instructions to request a web bug;

requesting the web bug sending a cookie and an URL for the web page;

saving the cookie and the URL for the web page as an entry in an association table;

querying, providing the URL for the web page, the association table for the cookie in the entry containing the URL;

identifying another entries in the association table containing the cookie;

identifying, from those entries, the entry containing an URL for an identification service, the identification service managing resource data; and

locating a resource using the resource data.

15. (original) A computer readable medium having instructions for:

generating, upon request from a user, a web page having content for requesting a web bug from an association service as well as content for displaying controls for selecting production options;

querying the association service to identify an identity service with which the user is registered providing an URL for the generated web page;

obtaining the user's resource data from the identified identity service;

locating and accessing a document management service using the resource data;

providing additional content for the web page for displaying controls for selecting a document managed by the document management service; and

producing a document according to selections made through the web page.

16. (original) The medium of Claim 15, wherein:

the instructions for generating comprise instructions for generating a web page having instructions to request a web bug sending to the association service association data containing a cookie and an URL for the web page;

the medium having further instructions for saving the association data as an entry in an association table;

the instructions for querying further comprise instructions for identifying the cookie in the saved entry using the provided the URL, identifying other association data containing the identified cookie, and, from the other identified association data, acquiring an URL for the identity service; and

the instructions for obtaining the user's resource data comprise instructions for obtaining the user's resource data from the identified identity service using, at least in part, the acquired URL.

17. (original) A system for locating a resource, comprising:

an association module operable to query an association service, supplying a session identifier, in order to identify an identity service managing resource data; and

an application operable to:

provide an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface;

acquire resource data from an identity service identified by a query from the association module; and

locate the resource using the resource data.

18. (original) The system of Claim 17, wherein:

the application is further operable to provide the interface in the form of a web page having instructions to send association data containing a cookie and the URL for the provided web page; and

the association module is further operable to provide the URL and query the association service for an URL for the identity service.

19. (original) A document production system, comprising:

an association module operable to query an association service, supplying a session identifier in order to identify an identity service managing resource data; and

a document production application operable to:

provide an interface having content for sending association data containing a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;

acquire resource data from an identity service identifier identified by a query from the association module;

locate and access a document management service using the resource data; and

provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and

produce a document according to selections made through the interface.

20. (original) A system for locating a resource, comprising:

an identity service operable to manage resource data;

an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;

an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using a session identifier supplied with the query;

an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;

an application operable to:

provide an interface having instructions to send association data to an association server, the association data to contain a client identifier and a session identifier for the provided interface;

acquire resource data from the identity service identified by a query from the association module; and

locate the resource using the resource data.

21. (original) The system of Claim 20, wherein:

the application is further operable to provide the interface in the form of a web page having instructions to send association data containing a cookie and the URL for the provided web page;

the association module is further operable to provide the URL interface and query the association service for an URL for the identity service; and

the association table interface is further operable to locate an entry in the association table containing the provided URL, identify the cookie in the located entry,

identify other entries containing that cookie, and, from those other entries, acquire an URL for the identity service; and

the application is further operable to use the acquired URL to acquire resource data from the identity service.

22. (original) A document production system, comprising:

a document management service;

an identity service operable to manage resource data for locating and accessing the document management service;

an association server operable to receive association data containing a client identifier and a session identifier, save the association data in an association table, and receive queries for the association table;

an association table interface in communication with the association server and operable, according to a received query, to access from the association table a session identifier for the identity service using the session identifier supplied with the query;

an association module operable to query, supplying a session identifier, the association service in order to identify the identity service;

a document production application operable to:

provide an interface having content for sending association data containing a client identifier and a session identifier for the provided interface to an association service as well as content for displaying controls for selecting production options;

acquire resource data from an identity service using the session identifier for the identity service identified by a query from the association module;

locate and access the document management service using the resource data;

provide, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and

produce a document according to selections made through the interface.

23. (original) The system of Claim 22, wherein:

the association table interface is further operable to locate an entry in the association table containing the session identifier supplied with a query, identify the client identifier in the located entry, identify other entries containing that client identifier, and, from those other entries, acquire a session identifier for the Identity service; and

the document production application is further operable to use the acquired session identifier for the identity service to acquire resource data from the identity service.

24. (original) A system for locating a resource, comprising:

a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data;

a means for providing an interface having instructions to send association data to the association service, the association data to contain a client identifier and a session identifier for the provided interface;

a means for acquiring resource data from an identity service identified by a query; and

a means for locating the resource using the resource data.

25. (original) A document production system, comprising:

a means for querying, supplying a session identifier, an association service in order to identify an identity service managing resource data;

a means for providing an interface having content for sending association data containing a session identifier for the provided interface to the association service as well as content for displaying controls for selecting production options;

a means for acquiring resource data from an identity service identifier identified by a query;

a means for locating and accessing a document management service using the resource data;

a means for providing, for the interface, additional content for displaying controls for selecting a document managed by the document management service; and

a means for producing a document according to selections made through the interface.